二分モーメントグラフによる除算表現の大きさの指数下界 (アルゴリズムと計算の理論)

AUTHOR(S):

中西, 正樹; 浜口, 清治; 柏原, 敏伸

CITATION:

中西, 正樹 ...[et al]. 二分モーメントグラフによる除算表現の大きさの指数下界 (アルゴリズムと計算の理論). 数理解析研究所講究録 1998, 1041: 63-70

ISSUE DATE:

1998-04

URL:

http://hdl.handle.net/2433/62070

数理解析研究所講究録
1041 巻 1998 年 63-70

二分モーメントグラフによる除算表現の大きさの指数下界

中西正樹 浜口清治 柏原敏伸
(Masaki Nakanishi) (Kiyoharu Hamaguchi) (Toshinobu Kashiwabara)
大阪大学大学院基礎工学研究科
E-mail: {m-naka/hama/kashi}@ics.es.osaka-u.ac.jp

Abstract

算術演算回路の設計検証のため提案された二分モーメントグラフは，$\{0,1\}$ のベクトルから整数への関数 $(f:\{0,1\}^n \to Z)$ を表す非巡回有向グラフである．また，マルティプリカティブ二分モーメントグラフは二分モーメントグラフの辺に重みを与えたものである．マルティプリカティブ二分モーメントグラフにおいては，加算や乗算などの関数を入力の桁数の多項式の大きさの節点数で表現できる．しかし，除算については節点数の下界が明らかにされていなかった．本稿では，二つの 2 進数の商を与える関数を表すマルティプリカティブ二分モーメントグラフの節点数の下界が指数関数になることを示す．

キーワード　二分モーメントグラフ，除算，下界

1 前書き

二分決定グラフ (Binary Decision Diagram, BDD)[1, 2] は，論理関数の非巡回有向グラフによる表現であり，実用的な論理関数の多くを比較的少ない記憶容量で表現できる．BDD は与えられた変数順序によってその大きさが変化するが，乗算 [3]，除算 [7] の (特定のビットの) 表現の大きさの下界は入力の桁数の指数関数になることが知られており，算術演算の表現には不適当であった．そこで，Bryant らは算術演算を効率的に表現するために，二分モーメントグラフを導入した．

二分モーメントグラフは，二分決定グラフと同様に関数の非巡回有向グラフによる表現であり，$\{0,1\}$ のベクトルから整数への関数 $(f:\{0,1\}^n \to Z)$ を表す．また，マルティプリカティブ二分モーメントグラフ (Multiplicative Binary Moment Diagram, *BMD)[4] は BMD の辺に重みを与えたものであり，乗算をはじめとする実用的な関数の多くについて入力の桁数の多項式に比例する大きさで表現できる [4] ことから，算術演算回路の設計検証の分野で用いられている [4, 5, 6]．しかし，*BMD による除算表現の大きさについては，実験的にその下界が入力の桁数の指数関数になるであろうと予想されているにすぎなかった．本稿では，*BMD による商表現の大きさの下界が入力の桁数の指数になることを証明する．

以下では，まず，2 節で下界を示すのに有用なフーリング集合という概念を説明し，フーリング集合の要素数と*BMD の節点数の関係を示す．次に 3 節で 2 数の商を与える関数を表す*BMD の節点数の下界が，$\Omega(2^{\frac{n}{24}})$ になることを示す．

2 準備

2.1 二分モーメントグラフ

二分モーメントグラフ (Binary Moment Diagram, BMD) は {0,1} のベクトルから整数への関数

$$\{0,1\}^m \to Z$$

を表す非巡回有向グラフである．

二分モーメントグラフは m 個の変数名のそれぞれが割り当てられた変数節点と整数値が割り当てられた定数節点を持ち，各節点は $\{0,1\}$ のベクトルから整数への関数を表す．変数節点には 0-枝，moment-枝と呼ばれる辺が接続しており，それらは他の節点を指している．変数節点 vについて，vの表す関数，v に割り当てられた変数名，vの 0-枝の指す節点，vの moment-枝の指す節点をそれぞれ $f[v]$, $index(v)$, $low(v)$, $moment(v)$，また，二分モーメントグラフの根となる節点を $root$ と表記する．

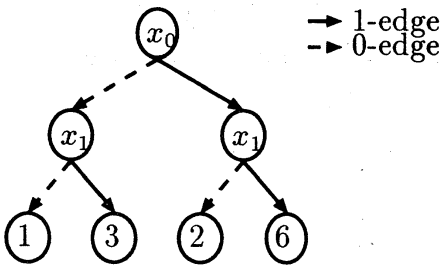
変数の順序πが存在し，根から定数節点に至るすべての経路中に出現する変数名の順序は，πに従う．すなわち，変数の集合 $\{z_1, z_2, \ldots, z_m\}$ に対して$\pi = (z_{k_1} < z_{k_2} < \ldots < z_{k_m})$ (ただし，$(k_1, \ldots, k_m)$ は $(1, \ldots, m)$ の置換) が与えられたとすると，z_{k_i}, z_{k_j} $(i < j)$ について，根から定数節点へ至る任意の経路上において，z_{k_i}は z_{k_j}より先に出現するということである．

二分モーメントグラフの各節点が表す関数 $f[v]$ の間には，以下のような関係がある．

$$f[low(v)] = f[v]|_{index(v)=0}$$
$$f[moment(v)] = f[v]|_{index(v)=1} - f[v]|_{index(v)=0}$$

ただし，$f[v]|_{x=a}$は $f[v]$ の変数 x に a を代入して得ら

れる関数を表すものとする．また，定数節点は，その節点に割り当てられた整数値をとる定数関数を表すものとする．$f[root]$ をその二分モーメントグラフが表す関数と定義する．(図 1)



$$f[root] = 6x_0x_1 + 2x_0 + 3x_1 + 1,\ \pi = (x_0 < x_1)$$

図 1: BMD の例

2.2 マルチプリカティブ二分モーメントグラフ

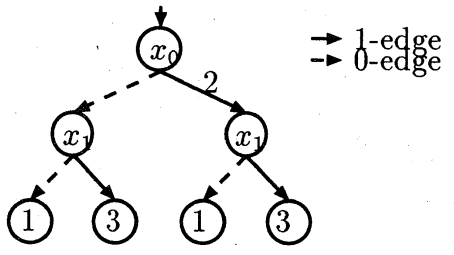
マルチプリカティブ二分モーメントグラフ (Multiplicative Binary Moment Diagram, *BMD) は二分モーメントグラフの辺に整数重みを与えたものである．節点 v の 0-枝，moment-枝に割り当てられた整数重みをそれぞれ $0\text{-}weight(v)$，$moment\text{-}weight(v)$ と表記する．また，根を指す辺を考え，その辺に割り当てられた整数重みを $root\text{-}weight$ と表記する．

マルチプリカティブ二分モーメントグラフの各節点が表す関数の間には，以下のような関係がある．

$$f[low(v)] = \frac{f[v]|_{index(v)=0}}{0\text{-}weight(v)}$$

$$f[moment(v)] = \frac{f[v]|_{index(v)=1} - f[v]|_{index(v)=0}}{moment\text{-}weight(v)}$$

$root\text{-}weight \cdot f[root]$ をマルチプリカティブ二分モーメントグラフが表す関数と定義する．(図 2)



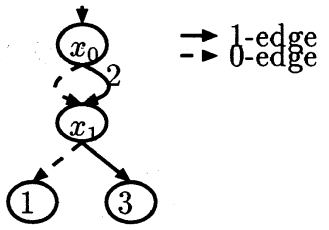
$$f[root] = 6x_0x_1 + 2x_0 + 3x_1 + 1,\ \pi = (x_0 < x_1)$$

図 2: *BMD の例

以下，本報告書では，二分モーメントグラフ，マルチプリカティブ二分モーメントグラフをそれぞれ BMD，*BMD と表記する．

また，BMD，*BMD 中の節点について，同じ関数を表す節点どうしは共有が可能である．(図 3)

このように，節点を共有させたグラフも BMD，*BMD と呼ぶ．一つの変数順序 π について同じ関数を表す BMD，



$$f[root] = 6x_0x_1 + 2x_0 + 3x_1 + 1,\ \pi = (x_0 < x_1)$$

図 3: *BMD における節点の共有の例

*BMD は一意とは限らないことになる．通常，適当な規則を付加することによって，変数順序に対してグラフを一意に決めることが可能である [4] が，本稿では下界を証明することが目的なので，そのような規則を考えない．

*BMD(と π) が与えられると，それが表す関数は一意に定まる．逆に $\{z_1, z_2, \ldots, z_m\}$ を変数とする関数 $f : \{0,1\}^m \rightarrow Z$ および順序 π が与えられたとする．f を表す*BMD は順序 π について (一意とは限らないが) 存在する．このような*BMD の性質を記述するために，以下，いくつかの定義を行う．

2.3 割当および l-項

関数 f を表す*BMD について，入力変数の集合 $Z = \{z_1, z_2, \ldots, z_m\}$，根から定数節点への経路上に出現する変数順序 $\pi = (z_{k_1} < z_{k_2} < \ldots < z_{k_m})$(ただし，$(k_1, \ldots, k_m)$ は $(1, \ldots, m)$ の置換) とする．

f をもとにいくつかの関数を定義するが，そのとき，変数 z_j に値 0 または 1 を代入することを行う．(結果として変数の個数の少ない関数が得られる．) このことを z_j への (値の) 割り当てと呼ぶ．ある i について $L = \{z_{k_1}, z_{k_2}, \ldots, z_{k_i}\}$ のすべての変数に対しての割り当てを左割当と呼び，L を (対応する) 左分割と呼ぶ．$z_{k_1}, z_{k_2}, \ldots, z_{k_i}$ に割り当てられた値をそれぞれ $a_1, a_2, \ldots, a_i$ とするとき，この左割当を $l = (a_1, a_2, \ldots, a_i)$ と表記する．$\{0,1\}$ ベクトル l 自体も左割当と呼ぶことにする．左割当 l における変数 z_j の値を (定義されているなら) $l(z_j)$ と表記する．例えば，$l(z_{k_2}) = a_2$ である．便宜上何も割り当てない場合も左割当と考え，$l = \varepsilon$ と表記する．さらに，$R = \{z_{k_{i+1}}, z_{k_{i+2}}, \ldots, z_{k_m}\}$ に対する値の割り当てを (適合する) 右割当と呼び，R を (適合する) 右分割と呼ぶ．また，左割当 l，適合する右割当 r を同時に行う割り当てを $l \cdot r$ と表記する．

f に左割当 l をほどこしたもの，すなわち各変数に l に従って値を代入して得られる関数を f の l-代入と呼び，$f^{l,\pi}$ と表記する．また，f に対して全ての変数に対する割り当て a を，ほどこしたもの (すなわち，l-代入の特別な場合) を $f(a)$ と表す．

左割当 l に対して l-項なるものを再帰的に次のように定義する．

- $l = \varepsilon$ のとき
$$f_\varepsilon^\pi = f$$
- $l \neq \varepsilon$ のとき
$l = (a_1, a_2, \ldots, a_i)$ のとき $l' = (a_1, a_2, \ldots, a_{i-1})$

とおいて

$$f_l^\pi = \begin{cases} f_{l'}^\pi|_{z_{k_i}=0} & (a_i = 0 \text{ のとき}) \\ f_{l'}^\pi|_{z_{k_i}=1} - f_{l'}^\pi|_{z_{k_i}=0} & (a_i = 1 \text{ のとき}) \end{cases}$$

以後，簡単のため，$f^{l,\pi}$，f_l^πをそれぞれ f^l，f_lと表記する．

補題 1 関数 f，順序πについて，lを左割当とする．関数 f を表す*BMD (変数の順序がπに従うもの) において，根を出発点とし，節点に対応付けられている変数に割り当てられた値が lにおいて 0 のときは 0-枝，1 のときは moment-枝を辿って行き着く節点を Vとする．このとき，0 でない整数 p が存在し，Vの表す関数を $\frac{f_l}{p}$ と表すことができる．

証明 定義より明らか． □

2.4 l-集合

左割当 l(すなわち $\{0,1\}$ のベクトル) に対し

$S_l = \{\hat{l} \mid \hat{l}$は$l$の 0 個以上の 1 を 0 に変えた左割当 $\}$

とおく．ただし，$l = \varepsilon$のときは $S_\varepsilon = \{\varepsilon\}$ と定める．S_lを l-集合と呼ぶ．例えば，$l = (101)$ のとき $S_{(101)} = \{(101),(100),(001),(000)\}$ となる．

2.5 l-項と l-集合の関係

割当 lの 1 の個数を lの重みと呼ぶことにし，関数 $Sign$ を次のように定義する．

$$Sign(l) = \begin{cases} 1 & (l\text{の重みが偶数}) \\ -1 & (l\text{の重みが奇数}) \end{cases}$$

特に $l = \varepsilon$の場合は重みは 0，$Sign(\varepsilon) = 1$ と定める．

l-代入より，符号 l-代入 f_s^lを次のように定義する．

$$f_s^l = Sign(l) \cdot f^l$$

次の補題が成り立つ．

補題 2 関数 fの l-項 f_lについて，

$$f_l = Sign(l) \cdot \sum_{\hat{l} \in S_l} f_s^{\hat{l}}$$

証明 変数名の順序を$\pi = (z_1 < z_2 < \ldots < z_m)$，左割当を $l = (a_1, a_2, \ldots, a_i)$ として一般性を失わない．lの重みを m とする．m についての帰納法で証明する．

$m = 0$ のとき ($l = \varepsilon$のときを含む)

$S_l = \{l\}$ より ($l = \varepsilon$のとき $S_\varepsilon = \{\varepsilon\}$ より)

$$\sum_{\hat{l} \in S_l} f_s^{\hat{l}} = f_s^l$$

よって，$f_l = f^l = f_s^l$より成り立つ．

$m = k$のときに成り立つと仮定する．

$m = k+1$ のとき

$a_i = 1$ の場合を示す．($a_i = 0$ の場合は後述)

$l' = (a_1, a_2, \ldots, a_{i-1})$ とする．

$$\begin{aligned} & f_l \\ = \; & f_{l'}|_{z_i=1} - f_{l'}|_{z_i=0} \\ & \qquad (f_l\text{の定義より}) \\ = \; & \left[Sign(l') \sum_{\hat{l'} \in S_{l'}} f_s^{\hat{l'}}|_{z_i=1}\right] \\ & - \left[Sign(l') \sum_{\hat{l'} \in S_{l'}} f_s^{\hat{l'}}|_{z_i=0}\right] \\ & \qquad (\text{帰納法の仮定より}) \\ = \; & Sign(l') \left[-\sum_{\hat{l} \in \{\hat{l} \mid \hat{l}(z_i)=1, \hat{l} \in S_l\}} f_s^{\hat{l}}\right] \\ & - Sign(l') \left[\sum_{\hat{l} \in \{\hat{l} \mid \hat{l}(z_i)=0, \hat{l} \in S_l\}} f_s^{\hat{l}}\right] \\ = \; & Sign(l) \sum_{\hat{l} \in S_l} f_s^{\hat{l}} \\ & \qquad (-Sign(l') = Sign(l) \text{ より}) \end{aligned}$$

次に，$a_i \neq 1$ の場合を考える．$a_j = 1$ となる jで最大のものを j_{max} とすると，左割当 $l'' = (a_1, a_2, \ldots, a_{j_{max}})$ について，上記の帰納法が適用できる．よって

$$f_{l''} = Sign(l'') \sum_{\hat{l} \in S_{l''}} f_s^{\hat{l}}$$

また，f_lの定義より

$$f_l = f_{l''}|_{z_{j_{max}+1}=0, z_{j_{max}+2}=0, \ldots, z_i=0}$$

よって

$$\begin{aligned} & f_l \\ = \; & f_{l''}|_{z_{j_{max}+1}=0, z_{j_{max}+2}=0, \ldots, z_i=0} \\ = \; & Sign(l'') \sum_{\hat{l} \in S_{l''}} f_s^{\hat{l}}|_{z_{j_{max}+1}=0, z_{j_{max}+2}=0, \ldots, z_i=0} \\ = \; & Sign(l) \sum_{\hat{l} \in S_l} f_s^{\hat{l}} \end{aligned}$$

よって，$a_i \neq 1$ の場合も補題が成り立つ． □

2.6 フーリング集合

集合 A が変数順序πについてのフーリング集合であるというのは，対応する左分割の等しいような左割当の集合であって，次のような条件を満たすときである．

任意の相異なる 2 つの左割当 $l, l' \in A$ に対して，

$$\begin{aligned} & \exists r \; f_l(r) = 0, f_{l'}(r) \neq 0 \\ or \quad & \exists r \; f_l(r) \neq 0, f_{l'}(r) = 0 \\ or \quad & \exists r, r' \; f_l(r) f_{l'}(r') \neq f_{l'}(r) f_l(r') \end{aligned}$$

ここで l，l'，f_l，$f_{l'}$はすべてπについてのものであり，r，r'は定まっていない全ての変数への割り当てである．(すなわち l，l'に適合する右割当である．このような右割当を A に適合する右割当と呼ぶ．)

フーリング集合の要素数と関数 fを表す*BMD の節点の個数に関して次の定理が成り立つ．

定理 1 関数 fについて，任意の変数順序πに対して要素数が c 個以上のフーリング集合が存在するとき，関数 fを表す任意の*BMD は少なくとも c 個の頂点を持つ．

証明 fを表す任意の*BMD を考え，それが持っている変数順序をπ，πについてのフーリング集合を A とする．任意の異なる 2 つの $l, l' \in A$ に対して，補題 1により決まる節点をそれぞれ P，Q とし，その節点の表す関数をそれぞれ $\frac{f_l}{p}$，$\frac{f_{l'}}{q}$とする．ここで p，qは補題 1によって決まる 0 でない整数である．

以下に $P \neq Q$ であることを示す．

- A に適合する右割当 rが存在して，$f_l(r) = 0$，$f_{l'}(r) \neq 0$ のとき
  $\frac{f_l(r)}{p}(= 0) \neq \frac{f_{l'}(r)}{q}(\neq 0)$，よって $P \neq Q$
- A に適合する右割当 rが存在して，$f_l(r) \neq 0$，$f_{l'}(r) = 0$ のとき
  $\frac{f_l(r)}{p}(\neq 0) \neq \frac{f_{l'}(r)}{q}(= 0)$．よって $P \neq Q$．
- Aに適合する右割当 r，r'が存在して，$f_l(r) \cdot f_{l'}(r') \neq f_{l'}(r) \cdot f_l(r')$ のとき
  $P = Q$ であると仮定すると，$\frac{f_l}{p}(r) = \frac{f_{l'}}{q}(r)$，$\frac{f_l}{p}(r') = \frac{f_{l'}}{q}(r')$

ゆえに $f_l(r)\cdot f_{l'}(r') = f_{l'}(r)\cdot f_l(r')$
これは矛盾である．よって $P \neq Q$ である．

したがって，fを表す*BMD 上には少なくとも $|A|$ 個の節点が存在する．よって補題が成り立つ． □

2.7 p-分離，分離ビット

関数 fの入力変数を $X \cup Y(X = \{x_{n-1},\ldots,x_0\}$, $Y = \{y_{n-1},\ldots,y_0\}$ (n は偶数)) とする．$X_U = \{x_{n-1},\ldots,x_{\frac{n}{2}}\}$, $X_D = \{x_{\frac{n}{2}-1},\ldots,x_0\}$ とおく．変数 $X\cup Y$の順序π，左分割 L，右分割 R が与えられたとして，$X_{UL} = X_U \cap L$, $X_{DL} = X_D \cap L$, $X_{UR} = X_U \cap R$, $X_{DR} = X_D \cap R$とおく．

整数 $p(1 \le p \le n-1)$ に対して，$Args_p$を次のように定義する．

$$Args_p = \{(x_a, x_b) | a - b = p, n-1 \ge a \ge \frac{n}{2}, \frac{n}{2} > b \ge 0\}$$

さらに p-分離 $Split_p$を次のように定義する．

$$Split_p = Args_p \cap [(X_{UL} \times X_{DR}) \cup (X_{UR} \times X_{DL})]$$

p-分離について次の補題が成り立つ．[3]

補題 3 $|X \cap L| = |X \cap R|$ のとき，ある p が存在して，$Split_p$は少なくとも$\frac{n}{8}$個の要素を含む．

以下，$|X \cap L| = |X \cap R|$ である分割 L，Rのみを考える．(この場合のみが後で必要になる．) 補題 3によって決まる p に対して s，t を次のように決める．(図 4)

$s = \frac{n}{2} - p, t = \frac{n}{2}$ $(p \le \frac{n}{2})$
$s = 0, t = p$ $(p > \frac{n}{2})$

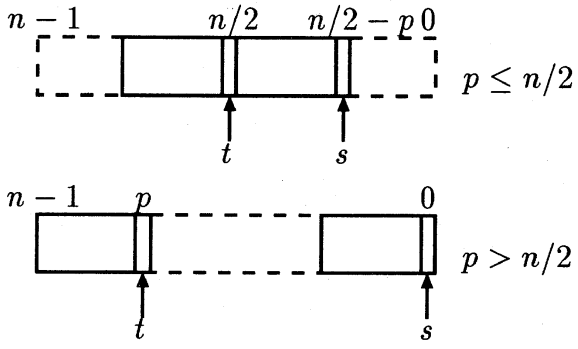


図 4: s，t の決め方

さらに，s'，t'を (もし存在するなら) 次のように決める．

$$s' = \min\{s' | t > s' \ge s, y_{s'} \in R\}$$
$$t' = \min\{t' | t' \ge t, y_{t'} \in R\}$$

分離上位 (下位) ビット $s_h(s_l)$ を次のように定義する．(図 5)

- $s' - s \ge t' - t$ もしくは s'が存在せず t'が存在するとき
$$s_l = s + (t' - t), s_h = t'$$
- $s' - s < t' - t$ もしくは t'が存在せず s'が存在するとき
$$s_h = t + (s' - s), s_l = s'$$
- t'，s'ともに存在しないとき
s_h，s_lともに定義されない．

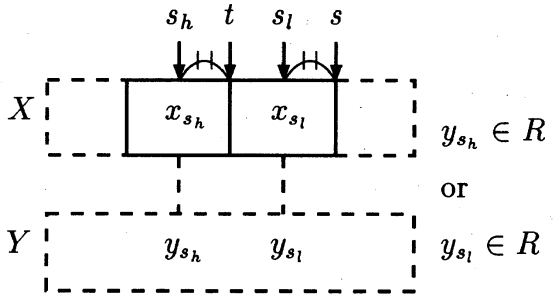


図 5: s_h，s_lの決め方

分離ビットをもとに，$Split'_p$を次のように定義する．

$$Split'_p = \begin{cases} Split_p \setminus \{(x_{s_h-i}, x_{s_l-i}) | 1 \le i \le s_h - t\} & (s_h, s_l\text{が定義されるとき}) \\ \emptyset & (s_h, s_l\text{が定義されないとき}) \end{cases}$$

次の補題が成り立つ．

補題 4 $x_i \in R$，$y_i \in L$ であるような x_i，y_iの組 (x_i, y_i) が，$|Split_p \setminus Split'_p|$ 個以上存在する．

証明 分離ビットの決め方より，$(x_u, x_d) \in Split_p \setminus Split'_p$ について，$y_u \in L$，$y_d \in L$ である．x_u，x_dのいずれか一方は Rに属するので補題が成り立つ． □

3 商を表現する*BMD の大きさの下界

$X = \{x_{n-1},\ldots,x_0\}$, $Y = \{y_{n-1},\ldots,y_0\}$ とし，$||X|| = 2^{n-1}x_{n-1} + 2^{n-2}x_{n-2} + \cdots + 2^0 x_0$, $||Y|| = 2^{n-1}y_{n-1} + 2^{n-2}y_{n-2} + \cdots + 2^0 y_0$とする．$f$は $X \cup Y$ を入力変数とし，$||X||$ を $||Y||$ で割った商を与える関数とする．

関数 fを表す*BMD について，次の定理が成り立つ．

定理 2 fを表す任意の*BMD について，その節点数は $\Omega(2^{\frac{n}{24}})$ である．

定理 2の証明の前に，補題を 2 つ示す．(変数順序πは任意とする)

補題 5 左割当 lに対して，lの重みが 1 以上のとき

$$\sum_{\hat{l} \in S_l} Sign(\hat{l}) = 0$$

証明 $\hat{l} \in S_l$の中で，重みが偶数のものの個数と，奇数のものの個数は等しい．よって補題が成り立つ． □

$X(a)$，$Y(a)$ をそれぞれ全変数への割当 a を行ったときの $||X||$，$||Y||$ の値とする．

補題 6 入力変数 $X \cup Y$，左割当 l，適合する右割当 rに対して，lの重みが 2 以上のとき

$$\sum_{\hat{l} \in S_l} X(\hat{l}\cdot r)\cdot Sign(\hat{l}) = 0$$

証明 割当$\hat{l}\cdot r$において変数 x_iに割り当てられている値を $x_i(\hat{l}\cdot r)$ と表記する．

$$\sum_{\hat{l} \in S_l} X(\hat{l}\cdot r)\cdot Sign(\hat{l})$$

$$= \sum_{\hat{l}\in S_l} \left(2^{n-1}x_{n-1}(\hat{l}\cdot r)+\cdots \right.$$
$$\left. \cdots + 2^0 x_0(\hat{l}\cdot r)\right) Sign(\hat{l})$$

となる．

$x_i \in R$のとき，$x_i(\hat{l}\cdot r)$は定数なので，補題5より

$$\sum_{\hat{l}\in S_l} 2^i x_i(\hat{l}\cdot r)Sign(\hat{l}) = 0$$

$x_i \in L$かつ$x_i(l\cdot r)=0$のとき，明らかに

$$\sum_{\hat{l}\in S_l} 2^i x_i(\hat{l}\cdot r)Sign(\hat{l}) = 0$$

$x_i \in L$かつ$x_i(l\cdot r)=1$のとき，$S_l^{x_i=1} = \{\hat{l}|\hat{l}\in S_l, \hat{l}(x_i)=1\}$，$S_l^{x_i=0} = \{\hat{l}|\hat{l}\in S_l, \hat{l}(x_i)=0\}$，

$$\begin{aligned}&\sum_{\hat{l}\in S_l} 2^i x_i(\hat{l}\cdot r)Sign(\hat{l})\\ &= \sum_{\hat{l}\in S_l^{x_i=1}} 2^i x_i(\hat{l}\cdot r)Sign(\hat{l})\\ &\quad + \sum_{\hat{l}\in S_l^{x_i=0}} 2^i x_i(\hat{l}\cdot r)Sign(\hat{l})\\ &= \sum_{\hat{l}\in S_l^{x_i=1}} 2^i x_i(\hat{l}\cdot r)Sign(\hat{l}) + 0\end{aligned}$$

lの重みが2以上であることより，$x_i=1$かつ重みが偶数の左割当 ($\hat{l}\in S_l$) の個数と，$x_i=1$かつ重みが奇数の左割当 ($\hat{l}\in S_l$) の個数は等しい．よって

$$\sum_{\hat{l}\in S_l^{x_i=1}} 2^i x_i(\hat{l}\cdot r)Sign(\hat{l}) = 0$$

したがって，

$$\sum_{\hat{l}\in S_l} 2^i x_i(\hat{l}\cdot r)Sign(\hat{l}) = 0$$

以上より

$$\sum_{\hat{l}\in S_l} X(\hat{l}\cdot r)\cdot Sign(\hat{l}) = 0$$

□

次に定理2の証明を与える．

証明 nは48以上の偶数とする．nが奇数のときには，$x_{n-1}=0$，$y_{n-1}=0$とすることによって，$n-1$ビットどうしの除算を扱うことができることから，偶数のときの結果を用いて，$\Omega(2^{\frac{n-1}{24}})$の定数係数を無視することによって，$\Omega(2^{\frac{n}{24}})$を得ることができる．

fを表す任意の*BMDを考え，その変数順序がπであるとする．$|X\cap L| = |X\cap R|$なる左分割L，右分割Rを一つ考える．(存在は自明)

補題3より，あるpについて$|Split_p| \geq \frac{n}{8}$である．以下，この$p$について考える．また，割当$a$において全ての割り当てが0のとき，$a=\bar{0}$と表記する．

(I) $|Split'_p| \geq \frac{n}{12}$の場合

(i) $|Split'_p \cap (X_{UL}\times X_{DR})| \geq |Split'_p \cap (X_{UR}\times X_{DL})|$の場合

$Split''_p = Split'_p \cap (X_{UL}\times X_{DR})$とおく．このとき，$|Split'_p| \geq \frac{n}{12}$，$|Split'_p \cap (X_{UL}\times X_{DR})| \geq |Split'_p \cap (X_{UR}\times X_{DL})|$より，$|Split''_p| \geq \frac{n}{24}$である．

集合Aを以下の条件を満たす左割当の集合とする．

$x \in \{x_u|(x_u,x_d)\in Split''_p\} = B$なる$x$について，

- xがBの要素中で最下位のものであるとき(このxをx_qとする)，x_qに1が割り当てられている．
- $x \in B\setminus\{x_q\}$なるxについて，任意の値が割り当てられている．ただし，x_qを含め少なくとも2つの$x\in B$に1が割り当てられている．

$y_{s_h}, y_{s_l} \in Y$について

- $y_{s_h}\in L$のとき，y_{s_h}に1が割り当てられている．
- $y_{s_l}\in L$のとき，y_{s_l}に1が割り当てられている．

上記以外のLに属する入力変数については，0が割り当てられている．

このとき，$|A| \geq 2^{\frac{n}{24}-1}-1$であることが容易にわかる．

以下，Aがフーリング集合であることを示す．

$\forall l, l' \in A (l\neq l')$について考える．$X(l\cdot\bar{0}) > X(l'\cdot\bar{0})$として一般性を失わない．右割当$r$を次のように与える．

- $y_{s_h}\in R$のとき，y_{s_h}に1を割り当てる．
- $y_{s_l}\in R$のとき，y_{s_l}に1を割り当てる．
- 左割当lにおいて$x_{i+s_h-s_l}$に1が割り当てられている(つまり$l(x_{i+s_h-s_l})=1$)とき，rにおいてx_iに1を割り当てる．ただし，$i+s_h-s_l=q$のときは，$l(x_{i+s_h-s_l})$の値に関わらずx_iに0を割り当てる．
- 他のRに属する入力変数については0を割り当てる．

X												
変数	x_{11}	x_{10}	x_9	x_8	x_7	x_6	x_5	x_4	x_3	x_2	x_1	x_0
分割	L	L	R	L	L	L	R	R	R	R	L	R
割当	1	1	0	0	0	1	1	1	0	0	0	0
Y												
変数	y_{11}	y_{10}	y_9	y_8	y_7	y_6	y_5	y_4	y_3	y_2	y_1	y_0
割当	0	0	0	0	0	1	0	0	0	0	0	1

$Split''_p = \{(x_{11},x_5),(x_{10},x_4),(x_8,x_2),(x_6,x_0)\}$,
$s_h=6$, $s_l=0$, $q=6$

図6: 割り当ての例

このrについて考える．(図6)

$y_{s_h}\in R$かつ$y_{s_l}\in R$の場合

$\forall \hat{l}\in S_l\ (\hat{l}\neq l)$について

$$0 \leq \frac{X(\hat{l}\cdot\bar{0})}{2^{s_h}} \leq \frac{X(\bar{0}\cdot r)}{2^{s_l}}$$

上式より，

$$\begin{aligned}&X(\hat{l}\cdot r) - (2^{s_h}+2^{s_l})\frac{X(\hat{l}\cdot\bar{0})}{2^{s_h}}\\ =\ &(X(\hat{l}\cdot\bar{0})+X(\bar{0}\cdot r))\\ &\quad -(X(\hat{l}\cdot\bar{0})+\frac{2^{s_l}}{2^{s_h}}X(\hat{l}\cdot\bar{0}))\\ =\ &X(\bar{0}\cdot r)-\frac{2^{s_l}}{2^{s_h}}X(\hat{l}\cdot\bar{0})\\ \begin{cases}\geq\\ \leq\end{cases}\ &\begin{matrix}X(\bar{0}\cdot r)-X(\bar{0}\cdot r)=0\\ X(\bar{0}\cdot r)<2^{s_h}+2^{s_l}\end{matrix}\end{aligned}$$

よって

$$2^{s_h}+2^{s_l} > X(\hat{l}\cdot r) - (2^{s_h}+2^{s_l})\frac{X(\hat{l}\cdot\bar{0})}{2^{s_h}} \geq 0$$

したがって，$X(\hat{l}\cdot r)$を$Y(\hat{l}\cdot r)=2^{s_h}+2^{s_l}$で割ったときの商$f^{\hat{l}}(r)$は

$$f^{\hat{l}}(r) = \frac{X(\hat{l}\cdot\bar{0})}{2^{s_h}}$$

また，$\hat{l}=l$のとき

$$(2^{s_h}+2^{s_l})\frac{X(l\cdot\bar{0})}{2^{s_h}} = X(l\cdot r) + 2^{q-(s_h-s_l)}$$

$2^{s_h}+2^{s_l} > 2^{q-(s_h-s_l)} > 0$より，$X(l\cdot r)$を$Y(l\cdot r)=2^{s_h}+2^{s_l}$で割ったときの商$f^l(r)$は

$$f^l(r) = \frac{X(l\cdot\bar{0})}{2^{s_h}} - 1$$

よって，補題2より

$$\begin{aligned} f_l(r) &= Sign(l)\sum_{\hat{l}\in S_l} f_s^{\hat{l}}(r) \\ &= Sign(l)\left[\left\{\sum_{\hat{l}\in S_l} Sign(\hat{l})\frac{X(\hat{l}\cdot\bar{0})}{2^{s_h}}\right\} \right. \\ &\quad \left. - Sign(l)\cdot 1\right] \end{aligned}$$

補題6より

$$f_l(r) = -Sign(l)^2 = -1$$

同様に，$\hat{l'}\in S_{l'}$について

$$0 \le \frac{X(\hat{l'}\cdot\bar{0})}{2^{s_h}} \le \frac{X(\bar{0}\cdot r)}{2^{s_l}}$$

より，$X(\hat{l'}\cdot r)$を$Y(\hat{l'}\cdot r) = 2^{s_h}+2^{s_l}$で割ったときの商$f^{\hat{l'}}(r)$は

$$f^{\hat{l'}}(r) = \frac{X(\hat{l'}\cdot\bar{0})}{2^{s_h}}$$

よって，補題2より

$$\begin{aligned} f_{l'}(r) &= Sign(l')\sum_{\hat{l'}\in S_{l'}} f_s^{\hat{l'}}(r) \\ &= Sign(l')\sum_{\hat{l'}\in S_{l'}} Sign(\hat{l'})\frac{X(\hat{l'}\cdot\bar{0})}{2^{s_h}} \end{aligned}$$

補題6より

$$f_{l'}(r) = 0$$

$y_{s_h}\in L$もしくは$y_{s_l}\in L$の場合（y_{s_h}，y_{s_l}の決め方より，少なくとも一方はRに属する．）

$S_l^{y_1} = \{\hat{l}|\hat{l}\in S_l, \hat{l}(y_{s_h}\in L) = 1 (or\ \hat{l}(y_{s_l}\in L) = 1)\}$，$S_l^{y_0} = \{\hat{l}|\hat{l}\in S_l, \hat{l}(y_{s_h}\in L) = 0 (or\ \hat{l}(y_{s_l}\in L) = 0)\}$，とすると，補題2より

$$\begin{aligned} f_l &= Sign(l)\sum_{\hat{l}\in S_l} f_s^{\hat{l}} \\ &= Sign(l)\left[\sum_{\hat{l}\in S_l^{y_1}} f_s^{\hat{l}} + \sum_{\hat{l}\in S_l^{y_0}} f_s^{\hat{l}}\right] \end{aligned}$$

$\sum_{\hat{l}\in S_l^{y_1}} f_s^{\hat{l}}$については，$y_{s_h}\in R$かつ$y_{s_l}\in R$の場合で示した結果を適用できる．よって

$$\begin{aligned} & f_l(r) \\ &= Sign(l)\left[\left\{\sum_{\hat{l}\in S_l^{y_1}} Sign(\hat{l})\frac{X(\hat{l}\cdot\bar{0})}{2^{s_h}}\right\}\right. \\ &\quad - Sign(l)\cdot 1 \\ &\quad \left. + \sum_{\hat{l}\in S_l^{y_0}} f_s^{\hat{l}}(r)\right] \\ &= Sign(l)\left[\left\{\sum_{\hat{l}\in S_l^{y_1}} Sign(\hat{l})\frac{X(\hat{l}\cdot\bar{0})}{2^{s_h}}\right\}\right. \\ &\quad - Sign(l)\cdot 1 \\ &\quad \left. + \begin{cases} \sum_{\hat{l}\in S_l^{y_0}} \frac{X(\hat{l}\cdot\bar{0})}{2^{s_h}} Sign(\hat{l})\Big] \\ (y_{s_h}\in R\text{つまり}, Y(\hat{l}\cdot r) = 2^{s_h}\text{のとき}) \\ \sum_{\hat{l}\in S_l^{y_0}} \frac{X(\hat{l}\cdot r)}{2^{s_l}} Sign(\hat{l})\Big] \\ (y_{s_l}\in R\text{つまり}, Y(\hat{l}\cdot r) = 2^{s_l}\text{のとき}) \end{cases} \end{aligned}$$

よって，補題6より

$$f_l(r) = -Sign(l)^2 = -1$$

同様に

$$f_{l'}(r) = 0$$

よってAはフーリング集合である．

(ii) $|Split'_p\cap(X_{UL}\times X_{DR})| < |Split'_p\cap(X_{UR}\times X_{DL})|$ の場合

$Split''_p = Split'_p\cap(X_{UR}\times X_{DL})$とおく．このとき，$|Split'_p|\ge\frac{n}{12}$，$|Split'_p\cap(X_{UL}\times X_{DR})| < |Split'_p\cap(X_{UR}\times X_{DL})|$より，$|Split''_p|\ge\frac{n}{24}$である．

集合Aを以下の条件を満たす左割当の集合とする．

$x\in\{x_d|(x_u,x_d)\in Split''_p\} = B$なる$x$について，

- xがBの要素中で最下位のものであるとき（このxをx_qとする），x_qに1が割り当てられている．
- $x\in B\setminus\{x_q\}$なるxについて，任意の値が割り当てられている．ただし，x_qを含め少なくとも2つの$x\in B$に1が割り当てられている．

$y_{s_h}, y_{s_l}\in Y$について

- $y_{s_h}\in L$のとき，y_{s_h}に1が割り当てられている．
- $y_{s_l}\in L$のとき，y_{s_l}に1が割り当てられている．

上記以外のLに属する入力変数については，0が割り当てられている．

このとき，$|A|\ge 2^{\frac{n}{24}-1}-1$であることが容易にわかる．

以下，Aがフーリング集合であることを示す．

$\forall l,l'\in A(l\ne l')$について考える．$X(l\cdot\bar{0}) > X(l'\cdot\bar{0})$として一般性を失わない．右割当$r$を次のように与える．

- $y_{s_h}\in R$のとき，y_{s_h}に1を割り当てる．
- $y_{s_l}\in R$のとき，y_{s_l}に1を割り当てる．
- 左割当lにおいて，x_iに1が割り当てられている（つまり$l(x_i)=1$）とき，rにおいて$x_{i+s_h-s_l}$に1を割り当てる．
- 他のRに属する入力変数については0を割り当てる．

X												
変数	x_{11}	x_{10}	x_9	x_8	x_7	x_6	x_5	x_4	x_3	x_2	x_1	x_0
分割	R	R	L	R	R	R	L	L	R	L	R	L
割当	1	1	0	0	0	1	1	1	0	0	0	1
Y												
変数	y_{11}	y_{10}	y_9	y_8	y_7	y_6	y_5	y_4	y_3	y_2	y_1	y_0
割当	0	0	0	0	0	1	0	0	0	0	0	1

$Split''_p = \{(x_{11},x_5),(x_{10},x_4),(x_8,x_2),(x_6,x_0)\}$，
$s_h = 6,\ s_l = 0,\ q = 0$

図7: 割り当ての例

このrについて考える．（図7）

$y_{s_h}\in R$かつ$y_{s_l}\in R$の場合

$\forall\hat{l}\in S_l\ (\hat{l}\ne l)$について

$$\frac{X(\hat{l}\cdot\bar{0})}{2^{s_l}} < \frac{X(\bar{0}\cdot r)}{2^{s_h}} < \frac{2^{s_h}+2^{s_l}}{2^{s_l}}$$

上式より，

$$\begin{aligned} & X(\hat{l}\cdot r) - (2^{s_h}+2^{s_l})\frac{X(\bar{0}\cdot r)}{2^{s_h}} \\ &= (X(\hat{l}\cdot\bar{0}) + X(\bar{0}\cdot r)) \\ &\quad - (X(\bar{0}\cdot r) + \frac{2^{s_l}}{2^{s_h}}X(\bar{0}\cdot r)) \\ &= X(\hat{l}\cdot\bar{0}) - \frac{2^{s_l}}{2^{s_h}}X(\bar{0}\cdot r) \\ &\begin{cases} < & X(\hat{l}\cdot\bar{0}) - X(\hat{l}\cdot\bar{0}) = 0 \\ > & X(\hat{l}\cdot\bar{0}) - (2^{s_h}+2^{s_l}) \ge -(2^{s_h}+2^{s_l}) \end{cases} \end{aligned}$$

よって

$$-(2^{s_h}+2^{s_l}) \le X(\hat{l}\cdot r) - (2^{s_h}+2^{s_l})\frac{X(\bar{0}\cdot r)}{2^{s_h}} < 0$$

したがって，$X(\hat{l}\cdot r)$ を $Y(\hat{l}\cdot r)=2^{s_h}+2^{s_l}$ で割ったときの商 $f^{\hat{l}}(r)$ は

$$f^{\hat{l}}(r) = \frac{X(\bar{0}\cdot r)}{2^{s_h}} - 1$$

また，$\hat{l}=l$のとき

$$(2^{s_h}+2^{s_l})\frac{X(\bar{0}\cdot r)}{2^{s_h}} = X(l\cdot r)$$

よって，$X(l\cdot r)$ を $Y(l\cdot r)=2^{s_h}+2^{s_l}$ で割ったときの商 $f^{l}(r)$ は

$$f^{l}(r) = \frac{X(\bar{0}\cdot r)}{2^{s_h}}$$

よって，補題2より

$$\begin{aligned} f_l(r) &= Sign(l)\sum_{\hat{l}\in S_l} f_s^{\hat{l}}(r) \\ &= Sign(l)\left[\left\{\sum_{\hat{l}\in S_l} Sign(\hat{l})\left(\frac{X(\bar{0}\cdot r)}{2^{s_h}}-1\right)\right\} \right. \\ &\quad \left. + Sign(l)\cdot 1\right] \end{aligned}$$

$\frac{X(\bar{0}\cdot r)}{2^{s_h}}-1$ は定数なので，補題5より

$$f_l(r) = Sign(l)^2 = 1$$

同様に，$\hat{l'}\in S_{l'}$について

$$\frac{X(\hat{l'}\cdot\bar{0})}{2^{s_l}} < \frac{X(\bar{0}\cdot r)}{2^{s_h}} < \frac{2^{s_h}+2^{s_l}}{2^{s_l}}$$

より，$X(\hat{l'}\cdot r)$ を $Y(\hat{l'}\cdot r)=2^{s_h}+2^{s_l}$ で割ったときの商 $f^{\hat{l'}}(r)$ は

$$f^{\hat{l'}}(r) = \frac{X(\bar{0}\cdot r)}{2^{s_h}} - 1$$

よって，補題2より

$$\begin{aligned} f_{l'}(r) &= Sign(l')\sum_{\hat{l'}\in S_{l'}} f_s^{\hat{l'}}(r) \\ &= Sign(l')\sum_{\hat{l'}\in S_{l'}} Sign(\hat{l'})\left(\frac{X(\bar{0}\cdot r)}{2^{s_h}}-1\right) \end{aligned}$$

$\frac{X(\bar{0}\cdot r)}{2^{s_h}}-1$ は定数なので，補題5より

$$f_{l'}(r) = 0$$

$y_{s_h}\in L$ もしくは $y_{s_l}\in L$ の場合 (y_{s_h}，y_{s_l}の決め方より，少なくとも一方はRに属する．)

$S_l^{y_1} = \{\hat{l}|\hat{l}\in S_l, \hat{l}(y_{s_h}\in L)=1 (or\ \hat{l}(y_{s_l}\in L)=1)\}$，$S_l^{y_0} = \{\hat{l}|\hat{l}\in S_l, \hat{l}(y_{s_h}\in L)=0 (or\ \hat{l}(y_{s_l}\in L)=0)\}$，とすると，補題2より

$$\begin{aligned} f_l &= Sign(l)\sum_{\hat{l}\in S_l} f_s^{\hat{l}} \\ &= Sign(l)\left[\sum_{\hat{l}\in S_l^{y_1}} f_s^{\hat{l}} + \sum_{\hat{l}\in S_l^{y_0}} f_s^{\hat{l}}\right] \end{aligned}$$

$\sum_{\hat{l}\in S_l^{y_1}} f_s^{\hat{l}}$については，$y_{s_h}\in R$かつ $y_{s_l}\in R$の場合で示した結果を適用できる．よって

$$\begin{aligned} & f_l(r) \\ &= Sign(l)\left[\left\{\sum_{\hat{l}\in S_l^{y_1}} Sign(\hat{l})\left(\frac{X(\bar{0}\cdot r)}{2^{s_h}}-1\right)\right\}\right. \\ &\quad + Sign(l)\cdot 1 \\ &\quad \left. + \sum_{\hat{l}\in S_l^{y_0}} f_s^{\hat{l}}(r)\right] \\ &= Sign(l)\left[\left\{\sum_{\hat{l}\in S_l^{y_1}} Sign(\hat{l})\left(\frac{X(\bar{0}\cdot r)}{2^{s_h}}-1\right)\right\}\right. \\ &\quad \left. + Sign(l)\cdot 1\right] \\ &\quad + \left\{\begin{array}{l} \left.\sum_{\hat{l}\in S_l^{y_0}} \frac{X(\bar{0}\cdot r)}{2^{s_h}} Sign(\hat{l})\right] \\ (y_{s_h}\in R\text{つまり}, Y(\hat{l}\cdot r)=2^{s_h}\text{のとき}) \\ \left.\sum_{\hat{l}\in S_l^{y_0}} \frac{X(\hat{l}\cdot r)}{2^{s_l}} Sign(\hat{l})\right] \\ (y_{s_l}\in R\text{つまり}, Y(\hat{l}\cdot r)=2^{s_l}\text{のとき}) \end{array}\right. \end{aligned}$$

よって，補題5，補題6より

$$f_l(r) = Sign(l)^2 = 1$$

同様に

$$f_{l'}(r) = 0$$

よってAはフーリング集合である．

(II) $|Split'_p| < \frac{n}{12}$の場合

このとき補題4より，$x_i\in R$，$y_i\in L$となるx_i，y_iの組(x_i,y_i)が，$\frac{n}{8}-\frac{n}{12}=\frac{n}{24}$個以上存在する．

ここで，$x_i\in R$，$y_i\in R$であるような(x_i,y_i)が存在しなければ，$|L\cap X| < |R\cap X|$とすることによって$x_i\in R$，$y_i\in R$であるような(x_i,y_i)が1つ存在し，しかも$x_i\in R$，$y_i\in L$であるような(x_i,y_i)が$\frac{n}{24}-1$個以上存在するように分割L，Rを作り直すことができる．

上述のような$x_w\in R$，$y_w\in R$となるwが存在するとする．

集合Aを以下の条件を満たす左割当の集合とする．

- $x_i\in R$，$y_i\in L$であるy_iには任意の値が割り当てられている．
- 上記以外のLに属する入力変数については0が割り当てられている．

このとき，$|A|\ge 2^{\frac{n}{24}-1}$であることが容易にわかる．

以下，Aがフーリング集合であることを示す．

$\forall l,l'\in A(l\ne l')$について考える．

lとl'について，$y_i\in L$，$l(y_i)\ne l'(y_i)$となるy_iの中で，iの値が最小のものをy_qとする．$l(y_q)=0$，$l'(y_q)=1$として一般性を失わない．

左割当l''を次のように与える．

- $y_i\in Y\cap L$ $(i<q)$について，l (l')と同様の割り当て$(l''(y_i)=l(y_i)=l'(y_i))$を行う．
- 上記以外のLに属する入力変数については0を割り当てる．

変数	x_7	x_6	x_5	x_4	x_3	x_2	x_1	x_0
分割	L	R	R	R	R	R	L	R
割当	0	1	0	0	1	0	0	0

変数	y_7	y_6	y_5	y_4	y_3	y_2	y_1	y_0
分割	L	R	L	L	L	L	R	L
割当lr	0	1	0	1	0	1	0	1
割当$l'r$	0	1	1	0	1	1	0	1
割当$l''r$	0	1	0	0	0	1	0	1

$w=6$，$q=3$

図 8: 割り当ての例

右割当rを次のように与える．(図8)

- $x_w=1$，$y_w=1$，$x_q=1$を割り当てる．

- 上記以外の Rに属する入力変数については0を割り当てる.

ここで, $S_l^1 = \{\hat{l} \in S_l | \exists i \geq q, y_i \in L$ かつ$\hat{l}(y_i) = 1\}$, $S_l^0 = \{\hat{l} \in S_l | \forall i \geq q, y_i \in L \Rightarrow \hat{l}(y_i) = 0\}$, 同様に $S_{l'}^1$, $S_{l'}^0$ を定義する. $S_l = S_l^1 \cup S_l^0$, $S_{l'} = S_{l'}^1 \cup S_{l'}^0$である.
すると

$$\forall \hat{l} \in S_l^1 \quad f^{\hat{l}}(r) = 0$$

$$\forall \hat{l'} \in S_{l'}^1 \quad f^{\hat{l'}}(r) = \begin{cases} 1\ (Y(\hat{l'} \cdot r) = 2^w + 2^q) \\ 0\ (\text{otherwise}) \end{cases}$$

また, $S_l^0 = S_{l'}^0 = S_{l''}$である.
よって, 補題2より

$$\begin{aligned} & f_l(r) \\ &= Sign(l) \sum_{\hat{l} \in S_l} f_s^{\hat{l}}(r) \\ &= Sign(l) \left[\sum_{\hat{l} \in S_l^1} f_s^{\hat{l}}(r) + \sum_{\hat{l} \in S_l^0} f_s^{\hat{l}}(r) \right] \\ &= Sign(l) \left[\sum_{\hat{l} \in S_l^1} 0 + \sum_{\hat{l} \in S_{l''}} f_s^{\hat{l}}(r) \right] \\ &= Sign(l) \sum_{\hat{l} \in S_{l''}} f_s^{\hat{l}}(r) \end{aligned}$$

$$\begin{aligned} & f_{l'}(r) \\ &= Sign(l') \sum_{\hat{l'} \in S_{l'}} f_s^{\hat{l'}}(r) \\ &= Sign(l') \left[\sum_{\hat{l'} \in S_{l'}^1} f_s^{\hat{l'}}(r) + \sum_{\hat{l'} \in S_{l'}^0} f_s^{\hat{l'}}(r) \right] \\ &= Sign(l') \left[-1 + \sum_{\hat{l} \in S_{l''}} f_s^{\hat{l}}(r) \right] \end{aligned}$$

右割当 r'を次のように与える. (図9)

- $x_w = 1$, $y_w = 1$を割り当てる.
- 上記以外の Rに属する入力変数については0を割り当てる.

変数	x_7	x_6	x_5	x_4	x_3	x_2	x_1	x_0
分割	L	R	R	R	R	R	L	R
割当	0	1	0	0	0	0	0	0

変数	y_7	y_6	y_5	y_4	y_3	y_2	y_1	y_0
分割	L	R	L	L	L	L	R	L
割当 lr'	0	1	0	1	0	1	0	1
割当 $l'r'$	0	1	1	0	1	1	0	1
割当 $l''r'$	0	1	0	0	0	1	0	1

$w = 6$, $q = 3$

図 9: 割り当ての例

このとき,

$\forall \hat{l_a} \in S_l \cup S_{l'}$
$Y(\hat{l_a} \cdot r') = 2^w$のとき (つまり$\hat{l_a} = \bar{0}$のとき)
$f^{\hat{l_a}}(r') = 1$
$Y(\hat{l_a} \cdot r') \neq 2^w$のとき
$f^{\hat{l_a}}(r') = 0$

よって, 補題2より

$$\begin{aligned} f_l(r') &= Sign(l) \sum_{\hat{l} \in S_l} f_s^{\hat{l}} \\ &= Sign(l) \cdot 1 \end{aligned}$$

同様に

$$f_{l'}(r') = Sign(l') \cdot 1$$

よって

$$f_l(r) f_{l'}(r') \neq f_{l'}(r) f_l(r')$$

よって Aはフーリング集合である.

以上より, 定理1から fを表す*BMD の節点数は$\Omega(2^{\frac{n}{24}})$である. □

4 後書き

本稿では, 割算の商を表す*BMD の節点数の下界が$\Omega(2^{\frac{n}{24}})$になることを示した. また, 同様な手法で, 割算の余りを表す*BMD の節点数の下界が$\Omega(2^{\frac{n}{24}})$になることも証明できる.

関数をグラフで表現する場合, どのようなグラフ表現を用いるかが節点数に大きな影響を与える. 例えば, 乗算を表現する場合 BDD では入力の桁数の指数関数に比例する節点数が必要なのに対し, *BMD では入力の桁数に比例する節点数で表現することが可能である.

関数のグラフ表現は算術演算回路の設計検証等への応用が考えられ, その性質の理論的解析が重要になると考えられる. したがって, 今後の課題として, 除算を*BMD 以外のグラフで表現した場合の下界の解析, 除算を多項式の大きさで表現するグラフ表現の考案等が挙げられる.

5 謝辞

本研究に関して, 貴重な御助言を頂いた木津隆史助手をはじめとする本学柏原研究室の方々に感謝致します.

参考文献

[1] S. B. Akers. "binary decision diagrams". *IEEE Trans. Comput.*, C-27(6):509–516, 1978.

[2] R. E. Bryant. "graph-based algorithms for boolean function manipulation". *IEEE Trans. Comput.*, C-35(8):677–691, 1986.

[3] R. E. Bryant. "on the complexity of VLSI implementations and graph representations of boolean functions with application to integer multiplication". *IEEE Trans. Comput.*, 40(2):205–213, 1991.

[4] R. E. Bryant and Y.-A. Chen. "verification of arithmetic circuits with binary moment diagrams". In *Proc. of 32nd Design Automation Conf.*, pages 535–541, 1995.

[5] Y.-A. Chen and R. E. Bryant. "ACV: An arithmetic circuit verifier". In *Proc. of ICCAD-96*, pages 361–365, 1996.

[6] K. Hamaguchi, A. Morita, and S. Yajima. "efficient construction of binary moment diagrams for verifying arithmetic circuits". In *Proc. of ICCAD-95*, pages 78–82, 1995.

[7] T. Horiyama and S. Yajima. "exponential lower bounds on the size of OBDDs representing integer division". In *Proc. of ISAAC'97*, pages 163–172, 1997.